6. References

1. F. Xia, L. T. Yang, L. Wang, and A. Vinel, “Internet of things,” International Journal of Communication Systems, vol. 25, no. 9, p. 1101, 2012.
2. O. Vermesan and P. Friess, “Internet of things: converging technologies for smart environments and integrated ecosystems”. River Publishers, 2013.
3. R. Li, T. Song, N. Capurso, J. Yu, J. Couture, and X. Cheng, “Iot applications on secure smart shopping system,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1945–1954, 2017.
4. (2020) The Growth in Connected IoT Devices.[Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213219
5. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, “Edge computing: Vision and challenges,” IEEE Internet of Things Journal, vol. 3, no. 5, pp.637–646, 2016.
6. M. Chiang and T. Zhang, “Fog and IoT: An overview of research opportunities,” IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854–864, 2016.
7. J. Pan and J. McElhannon, “Future edge cloud and edge computing for internet of things applications,” IEEE Internet of Things Journal, vol. 5, no. 1, pp. 439–449, 2017.
8. F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the internet of things,” in Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, 2012, pp. 13–16.
9. S. K. Lo, Y. Liu, S. Y. Chia, X. Xu, Q. Lu, L. Zhu, and H. Ning, “Analysis of blockchain solutions for IoT: A systematic literature review,” IEEE Access, vol. 7, pp. 58 822–58 835, 2019.
10. H.N. Dai, Z. Zheng, Y. Zhang, “Blockchain for Internet of Things: A Survey”, IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076 - 8094, 2019.
11. R. Yang, F. R.Yu, P. Si, Z. Yang, Y.Zhang, “Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges”, IEEE Communications Surveys & Tutorials, Vol.21, Issue 2, pp. 1508 – 1532,2019
12. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf (2008). Accessed 30 Aug 2019.

13. T.Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, T. Alghamdi, "A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations", IEEE Access, Vol. 7, pp. 176838 - 176869, 2019
14. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, 25-30 June 2017
15. M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?", IEEE Security & Privacy, vol. 16, no. 5, pp. 38-41, Sep./Oct. 2018.
16. T. M. Fernández-Caramès, P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks", IEEE Access, Vol.8, pp. 21091 – 21116, 2020.
17. Wu, F., Li, X., Xu, L., Kumari, S., Karuppiah, M., Shen, J. "A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server", Comput. Electr. Eng. 63, 168–181 (2017)
18. Gope, P., Sikdar, B., "Lightweight and privacy-preserving two factor authentication scheme for IoT devices". IEEE Internet of Things J. 6, 580–589 (2019)
19. Feng, W., Qin, Y., Zhao, S., Feng, D. "AAoT: lightweight attestation and authentication of low-resource things in IoT and CPS", Comput. Netw. 134, 167–182 (2018)
20. Roychoudhury, P., Roychoudhury, B., Saikia, D.K., "Provably secure group authentication and key agreement for machine type communication using Chebyshev's polynomial", Comput. Commun.127, 146–157 (2018)
21. Aman, M.N., Chua, K.C., Sikdar, B. "Mutual authentication in IoT systems using physical unclonable functions", IEEE Internet Things J. 4, 1327–1340 (2017)
22. Vijayakumar, P., Chang, V., Deborah, L.J., Balusamy, B., Shynu, P.G." Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks", Future Gener. Comput. Syst. 78, 943–955 (2018)
23. Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in Proc. IEEE Int. Conf. Serv.-Oriented Comput. Appl., 2014, pp. 230–234.
24. Alexaki, S., Alexandris, G., Katos, V., & Petroulakis, E. N.,"Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions", In 2018 IEEE 23rd

International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.

25. de Oliveira, M. T., Reis, L. H., Carrano, R. C., Seixas, F. L., Saade, D. C., Albuquerque, C. V., … & Ma.os, D. M. (2019, May), "Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications", In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
26. Chen, Y., Li, H., Li, K., & Zhang, J., "An improved P2P File system scheme based on IPFS and Blockchain". IEEE International Conference on Big Data, pp. 2652-2657. 2017.
27. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Working Paper, 2008, [Online] Available: https://bitcoin.org/bitcoin.pdf
28. [18] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, Vol. 151, pp. 1–32, 2014, [Online] Available: https://gavwood.com/paper.pdf
29. H-W. Wang, " On sharding blockchains,"Accessed on: Mar. 27, 2020, [Online] Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQ
30. "EOSIO." [Online]. Available: https://eos.io
31. "Zilliqa." [Online]. Available: https://zilliqa.com/
32. "Plasma." [Online]. Available: http://plasma.io/
33. L. Jiang, L. Da Xu, H. Cai, Z. Jiang, F. Bu, and B. Xu, "An iot-oriented data storage framework in cloud computing platform," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1443–1451, 2014.
34. M. Chen, S. Mao, and Y. Liu, "Big data: A survey," Mobile networks and applications, vol. 19, no. 2, pp. 171–209, 2014.
35. H. Cai, B. Xu, L. Jiang, at al. "IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges" in EEE Internet of Things Journal, vol. 4, no. 1, pp. 75-87, Feb 2017
36. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.
37. W. Shi and S. Dustdar, "The promise of edge computing," Computer, vol. 49, no. 5, pp. 78–81, 2016.

38. R. Roman, J. Lopez, and M. Mambo, “Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges,” Future Generation Computer Systems, vol. 78, pp. 680–698, 2018.
39. Z. Zheng, S. Xie, H. Dai, et al. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” 2017 IEEE International Congress on Big Data, Honolulu, HI, 2017, pp. 557-564.
40. K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.
41. A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and solutions," arXiv preprint arXiv:1608.05187, 2016.
42. S. Ali, G. Wang, M. Z. A. Bhuiyan, et al. “Secure Data Provenance in Cloud-Centric Internet of Things via Blockchain Smart Contracts,” 2018 IEEE SmartWorld, Guangzhou, 2018, pp. 991-998.
43. Ruinian Li, Tianyi Song, Bo Mei, Hong Li, Xiuzhen Cheng, Liming Sun, “Blockchain For Large-Scale Internet of Things Data Storage and Protection”, IEEE Transactions on Services Computing, Vol.12 , Issue 5, pp 762 – 771, 2019.
44. M. Satyanarayanan, “The emergence of edge computing,” Computer, vol. 50, no. 1, pp. 30–39, 2017.
45. F. Li, Y. Han, and C. Jin, “Certificateless online/offline signcryption for the internet of things,” Wireless Networks, vol. 23, no. 1, pp. 145–158, 2017.
46. Shaoyong Guo, Xing Hu, Song Guo, Xuesong Qiu, Feng Qi, “Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System”, IEEE Transactions on Industrial Informatics, Vol. 16 Issue 3, pp 1972 – 1983, 2020.
47. Zhao, H., Bai, P., Peng, Y., & Xu, R., “Efficient key management scheme for health blockchain”, CAAI Transactions on Intelligence Technology, 3(2), 114-118, 2018.
48. Zhang, X., Poslad, S., & Ma, Z., “Block-Based Access Control for Blockchain-Based Electronic Medical Records (EMRs) Query in eHealth”, IEEE Global Communications Conference, GLOBECOM, pp. 1-7, IEEE, Dec-2018.
49. K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, D. Song, R. Wattenhofer, and E. G. Sirer, ``On scaling decentralized blockchains," in Proc. Int. Conf. Financial Cryptogr. Data Secur. Christ Church, Barbados: Springer, 2016, pp. 106-125.

50. Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.
51. W. Gao, W. G. Hatcher, and W. Yu, “A survey of blockchain: Techniques, applications, and challenges,” in 2018 27th International Conference on Computer Communication and Networks (ICCCN), July 2018, pp. 1–11.
52. W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, “A survey on consensus mechanisms and mining strategy management in blockchain networks,” IEEE Access, vol. 7, pp. 22 328– 22 370, 2019
53. A. Hafid, A. S. Hafid, M. Samih, “A Methodology for a Probabilistic Security Analysis of Sharding-Based Blockchain Protocols,” in Proceedings of the International Congress on Blockchain and Applications, Springer, 2019, pp. 101–109.
54. M. Zochowski “A Highly Scalable Decentralized Transaction System,” Version 1.0, 2018, [Online] Available:https://logos.network/whitepaper.pdf
55. V. Buterin, “ Ethereum Sharding FAQ,” Accessed on: Jan. 28, 2020, [Online] Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQ
56. H. Dang, T. T. A. Dinh, D. Loghin, E. Chang, Q. Lin, and B. C. Ooi,“Towards scaling blockchain systems via sharding,” in Proceedings of the 2019 International Conference on Management of Data, ACM, 2019, pp. 123–140.
57. K. Lauter, ``Postquantum opportunities: Lattices, homomorphic encryption, and supersingular isogeny graphs," IEEE Security Privacy, vol. 15, no. 4, pp. 22-27, Aug. 2017.
58. R. L. Rivest, A. Shamir and L. M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978.
59. N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of Computation, vol. 48, no. 177, pp. 203-209, Jan. 1987.
60. V. S. Miller, “Use of elliptic curves in cryptography,” In Proceedings of Advances in Cryptology, LNCS 218, pp. 417-426, Aug. 1985.
61. W. Diffie and M. E. Hellman, “New directions in cryptography,”, IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.

62. National Institute of Standards and Technology (NIST), “FIPS 186-2: Digital Signature Standard (DSS)”, Jan. 2000.
63. P. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” SIAM Journal on Computing, vol. 26, no. 5, pp. 1484-1509, Oct. 1997.
64. L. K. Grover, “A fast quantummechanical algorithm for database search”. In Proc. 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, USA, May 1996.
65. M. Rückert, ``Lattice-based blind signatures," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., Dec. 2010, pp. 413-430.
66. M. Rückert, “Strongly unforgeable signatures and hierarchical identity based signatures from lattices without random oracles," in Proc. Int. Workshop Post-Quantum Cryptogr., May 2010, pp. 182_200.
67. S. Agrawal, D. Boneh, and X. Boyen, ``Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in Proc. Adv. Cryptol. Conf. CRYPTO, Santa Barbara, CA, USA, Aug. 2010, pp. 98_115.
68. J. Yan, L.Wang, M. Dong, Y. Yang, andW. Yao, ``Identity-based signcryption from lattices," Secur., Commun. Netw., vol. 8, no. 18, pp. 3751-3770, 2015.
69. Y. Gao, X. Chen, Y. Chen, Y. Sun, X. Niu, Y. Yang, “A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain”, The Internet of Energy: Architectures, Cyber Security, and Applications (Part II), IEEE Access, Vol.-6, pp. 27205 – 27213, 2018
70. G. Greenspan, MultiChain Private Blockchain-White Paper.Technical report, Coin Sciences Ltd (2015). http://www.multichain.com/download/MultiChain-White-Paper.pdf.
71. https://www.hyperledger.org/
72. https://www.r3.com/reports/corda-technical-whitepaper/
73. https://www.r3.com/wp-content/uploads/2019/06/corda-platform-whitepaper.pdf

Gmail **Suniel <sunielparihar@gmail.com>**

Fwd: [Urkund] 1% similarity - head-library@svvv.edu.in

1 message

Head Library <head-library@svvv.edu.in> 6 August 2020 at 15:30
To: Suniel <sunielparihar@gmail.com>, sunilparihar@svvv.edu.in

---------- Forwarded message ---------
From: <report@analysis.urkund.com>
Date: Thu, Aug 6, 2020 at 3:26 PM
Subject: [Urkund] 1% similarity - head-library@svvv.edu.in
To: <head-library@svvv.edu.in>

Document sent by: head-library@svvv.edu.in
Document received: 8/6/2020 11:54:00 AM
Report generated 8/6/2020 11:56:36 AM by Urkund's system for automatic control.

Student message: SUNEEL SYNO.

Document : Final Synopsis - Copy.docx [D77533061]

About 1% of this document consists of text similar to text found in 160 sources. The largest marking is 15 words long and is 88% similar to its primary source.

PLEASE NOTE that the above figures do not automatically mean that there is plagiarism in the document. There may be good reasons as to why parts of a text also appear in other sources. For a reasonable suspicion of academic dishonesty to present itself, the analysis, possibly found sources and the original document need to be examined closely.

Click here to open the analysis:
https://secure.urkund.com/view/74350790-664390-848283

Click here to download the document:
https://secure.urkund.com/archive/download/77533061-371133-801376

--
With regards

Dr. GHS Naidu
Chief Librarian
SVVV, Indore
Mob:9303330439

Document Information

Analyzed document	Final Synopsis - Copy.docx (D77533061)
Submitted	8/6/2020 11:54:00 AM
Submitted by	headlibrary
Submitter email	head-library@svvv.edu.in
Similarity	1%
Analysis address	headlibrary.svvv@analysis.urkund.com

Sources included in the report

W	URL: https://ruc.udc.es/dspace/bitstream/handle/2183/25176/T.M.Caram%C3%A9s_Towards_Pos ... Fetched: 8/6/2020 11:56:00 AM	2
W	URL: https://www.researchgate.net/publication/326215813_Blockchain_For_Large-Scale_Inte ... Fetched: 1/31/2020 12:30:13 PM	1
W	URL: https://www.researchgate.net/publication/328706514_Blockchain's_adoption_in_IoT_Th ... Fetched: 4/16/2020 8:49:32 AM	1

Entire Document

1. Introduction Internet of Things (IoT) is the term that provides the connections with the objects that are used in day to day life. As the deployment of the devices of IOT devices are increasing, which results in the higher interaction as well the accuracy and other aspects are improved tremendously [1, 2, 3]. International Data Corporation calculated that 41 billion IoT devices connected to the internet will be generated 79.4 zettabytes(ZB) of data by 2025. [4]. Huge amount of IOT devices that deployed brings various challenges to store and manage this large volume of data. In Cloud computing the networks are centrally managed, along with the data gathering on the outer edge and sent back for processing at the servers. This design become out the way that a large number of devices situated closed to edge did not have the computation power and storage capacity to process the information they gathered. Also more devices are able to connect with cellular and wifi, so the functions of these devices are limited as per the hardware attached. IOT device have low computing power and are not capable for complex calculations. Edge computing can be used to overcome these problems [5, 6, 7]. Edge computing is just a processing method for the data collected at the edges, replacing the cloud [8]. Edge computing provides real time communications and computation through close edge servers. An edge device can be any computing device that resides between data source and cloud. Another problem with traditional cloud-based IoT infrastructure is that a centralized server gets and manages all the data, which has a risk of the whole down system, if the centralized server is down. Also, personal data may be leaked from the available server as it is vulnerable to various forms of attack. For example server may trade important data without notifying the owner of data [9]. Present cloud-based IoT structure having a risk of single point of failure due to its centralized nature and also not capable to resist various forms of cyber attacks, a less vulnerable and decent approach is required to address these problems. Blockchain technology has shown a great opportunity to overcome the challenges faced by cloud-based IoT structure [10, 11]. Blockchain can be stated as the ledger that is distributed and spreading over the whole distributed system. As the blockchain is not a centralized system, the transactions can be carried out in a distributed way, without the involvement of trusted third party [12]. Whereas the traditional system handles the transaction at the central level and this central system provides the validity of the transaction. However blockchain save the cost and mitigate the problem of performance bottleneck at the central server by validation of transactions decentrally. Moreover every transaction in blockchain is immutable as the committed transactions are kept inside the every node that is present in network. Therefore, the blockchain can ensure non-repudiation of transactions. In addition, each transaction in blockchains is visible to every user with the attached historic timestamp. There are basically two types of blockchains; Private blockchain (called as permissioned blockchain) and public blockchain (called as permissionless blockchain). In a public blockchain, any outsider can be entered in the blockchain network, and transactions made over the public blockchain are fully transparent and made publically. In permissioned blockchain, permission is needed to get into it and all transactions made over permissioned blockchain are private and only available for the members of permissioned blockchain [13][14]. As the transactions increase over the blockchain network, it becomes the right place for various attackers to steal sensitive information. Trending technologies like quantum computing gives more power to these attackers. Quantum computing helps them to easily crack keys and get unauthorized access to the confidential information available over the network [15].To overcome this security concern the post-quantum cryptographic algorithms can be used in the blockchain that resists attacks made by quantum computers [16]. The IOT security deals with various dimensions i.e. integrity of data, confidentiality of data and no repudiation. Also we see that the authorization and the control for access handle the starting of defense that gives the access of data to the particulars with the correct data. There are several methods have been proposed for authentication of IoT devices [17-20]. The major issue with the current authentication scheme is that they use cryptographic techniques which bring key distribution problem and require high computations. Moreover, authentication data and keys are stored on a central server, which puts the system in risk of failure if the centralized server is down. Some authentication techniques [21, 22] require higher exchanges of messages between the devices and the server. So there is scope to improve the authentication mechanism for IoT devices over the blockchain network. Another challenge in traditional cloud-based IoT system is to guarantees the integrity of IoT data. Traditional data integrity schemes such as symmetric key approaches and Asymmetric key approaches suffer from the single-point downs the whole system and network congestion due to the centralized architecture [23].Some authors [24, 25] proposed on chain data storage scheme they didn't consider the case when the size of the data is vast for a blockchain ledger that causes low throughput and make blockchain network less efficient. Maintaining data integrity over the blockchain network without affecting throughput and scalability of network is still a challenging task. Blockchain methodology has used in large not only in IoT, as well in every industries. Blockchain gained this popularity just because it transparent, decentralized, immutable and whole distributed peer to peer architecture that stores the transactions. Apart from these selected attributes, the limitation of scalability is seen in the blockchain that is per second processing of transactions which is 7 for Bitcoin [27] and 15 for

Ethereum [28]. The scalability trilemma is as known in blockchain given by Vitalik Buterin, co-founder of Ethereum [29]. Vitalik said that the trade off are inevitable in between the major three properties that are scalability, decentralization and the security (Figure 1).

Figure 1

Decentralization is the essential behavior of blockchain; whereas security is a fundamental property, but the scalability is the major issue. We can say as, the scalability dilemma tells that at a time only two out of decentralization and security or the scalability. So, trade-offs are inevitable. Some of the solutions are presented in the literature for the scalability for permission blockchain [30, 31, 32]. However, they do not consider different users conditions, only using a single consensus protocol for all type of applications. So to enhance scalability and maintaining throughput and decentralization characteristic of the blockchain a better approach is required. Designing of IoT data storage framework over permissioned blockchain network is a challenging task. As the IoT devices have low resources, edge computing requires to be integrated so that data can be managed on the network edge, and the transaction can be created on behalf of IoT devices. The integrity of IoT data must be maintained efficiently so that it doesn't affect throughput and scalability property of blockchain. However, an entity required to access data; the blockchain should decide that the access can be granted or not to that entity, i.e., distributed blockchain miners will handle the authentication request in place of a centralized server. Blockchain network scalability is another challenging task, existing blockchain network works on single consensus protocol that makes it slow and less scalable, so there is the scope of scalable batter technique without affecting throughput and decentralized characteristic of blockchain. At last,

56% MATCHING BLOCK 1/4 W https://ruc.udc.es/dspace/bitstream/handl ...

the security of the blockchain is dependable on public-key cryptosystems and hash functions which are threatened by the evolution of quantum computers.

So to enhance the security of current blockchain network post-quantum computing cryptography techniques are required so that the blockchain network can resist the quantum computing attacks.

2. Literature Review In the last years, many researchers have made constructive efforts to develop several methodologies to store and protect IoT data. Also, many attempts have been undertaken to address the analysis of narrative work in Blockchain, post-quantum blockchain and IoT. Here in this section summary of the work done in this area is presented.

A data storage framework was proposed by Jiang et al. [33] that enable the efficient storage for the huge amount of data coming from the IoT devices; as well this system integrates the structured data and the unstructured data. The presented system for the storage of data is able to manage many databases and the extension of database, also hadoop for the storing and managing various types of data that are founded by the sensors.

M. Chen, S. Mao et al. [34] reviewed

87% MATCHING BLOCK 2/4 W https://www.researchgate.net/publication/ ...

the background and state-of-the-art of big data. . They first

bring in the common background of big data and review related technologies. In addition to that they have examined the some of the application that are found in big data environment such as the IOT, social network, medical field, etc. They have surveyed the problems of the big data storing and the security of data.

H. Cai et al. [35] worked for the some major areas of IOT big data like acquisition, management and the processing and mining of data. The authors have some of the models for these works have described by discussing their capacity and the characteristics In this paper, authors analysed recent research in IoT field, and also identified the issues and possibilities for the data storage and management for IoT devices.

W. Shi et al. [36] stated the edge computing and studies some of the cases that vary from the offloading of cloud to the city and homes. As well the authors have studied the collaborative edge for stating the edge computing concept. Also, in [37] describe the importance and need for edge computing. They discuss some open issues like programming challenges, Naming, Privacy and security regarding edge computing and the area where edge computing becomes prominent.

R. Roman, J. Lopez et al. [38] identified some of the common issues and some common features for every edge paradigm and analysed some of the threats for security of system and the challenges that are seen for this edge paradigm. They discussed the issues related to authentication, access control, trust management, intrusion detection and privacy in edge network.

Z. Zheng et al. [39] present a study on the blockchain methodology that includes architecture and key functionalities of blockchain. The regular algorithms for blockchain are discussed and comparison of this is done with protocols in various aspects. This paper also founded issues and the challenges faced by the blockchain development and at the end they summarized the approaches that are able for solving these problems.

In 2016, K. Christidis et al. [40] studied in their study how the blockchain may used for security purpose in the IoT domain. They also explained

100% MATCHING BLOCK 3/4 W https://www.researchgate.net/publication/ ...

how this mechanism works and also look into smart contracts.

They stated some of the IOT applications where the blockchain can be fitted; however, more specific solutions are expected.

A. Dorri et al. [41] presented an architecture of smart houses with IoT systems; This architecture is consist of overview of network and the storage on cloud for the coordination among the data and the transactions along with the blockchain for providing the safety and privacy. The presented scheme makes use of blockchains that depends on the transaction that is taking place in which network hierarchy and for this it uses the trust method that are distributed and in the topology without any central command.

S. Ali et al. [42] presented a framework that is secure and is centralized on cloud IOT network and for this it makes utilization of the blockchain properties that are immutable, deterministic and public, with the formal infrastructure of cloud. In their technique the blockchain contains the cryptographic hash of the metadata present in all the devices. In contrast, the real data is stored off-chain, which makes it more scalable for deploying the IOT devices.

Li et al. [43] proposed blockchain based mechanism for secure storage of data and providing protection to the data. Edge computing [44] works as for the computation at IOT devices and for managing the storage of data. This work uses certificates cryptography algorithm for authentication of IoT devices which is a public key cryptography algorithm. The proposed action does not address data integrity issue and also there is a scope for improvement in the authentication mechanism.

F. Li et al. [45] presented a new certificate online/offline sign encryption technique to authenticate IoT devices over the heterogeneous networks. On comparison with the two earlier available certifications online/offline sign encryption schemes, in the phase of online this particular scheme does not require any operation of point multiplication. This makes it more flexible with the resource constrained devices. In the offline phase the identity of the receiver is needed, and this limits this scheme.

S. Guo et al. [46] proposed a mechanism to improve the efficiency of authentication and for this they used the blockchain and edge computing technology. They have given a cryptographic method that is asymmetric for the security from attacks. The proposed method can be enhanced by introducing token-based authentication between blockchain and edge devices.

Fan et al. [17] stated a mechanism for the authentication which works on the wearable devices, smart phone and a server of cloud. The storage of devices is saved by storing the data on cloud. For the encryption they have used the symmetric key cryptography technique. The keys from symmetric cryptography are stored at the server so this makes is single point failure prone.

Gope et al. [18] given an two factor based authentication mechanism which is able to authenticate IOT devices as well the system gets the physical properties and saves them from physical attack. The data for the authentication is kept on the server that becomes the drawback of the system. Also the system requires exchanges of five messages from device to sever.

Feng et al. [19] have worked on the attestation from the remote location for the devices that are of either IOT or from the cyber physical system. The mechanism for this remote authentication is presented by authors who work on the basis of the physical characteristics of the devices. Whenever the device wants to get the authentication the signature is taken and matched with the server. Thus the mechanism is not efficient for the environments which have resource constrained devices.

Aman et al. [21] stated mechanism for authentication that is lightweight and does not store the secret key at the server located at centre. Physical Unclonable Functions (PUF) based mechanism is presented by authors, the functions of the physical devices based on the properties of physical devices and the impersonation is almost impossible. The system need to exchange five messages that makes it unreliable and inefficient for use.

Vijayakumaret al. [22] gave a mechanism for the end devices that need very less amount of information and by this the privacy can be improved. Short group signature scheme for sharing secrete by Shamir is used on this method. Problem seen in this method is that the secret key is needed to be stored in each device thus makes more storage. In addition to that the method requires a more message exchange for authentication.

In [24] [25], stated a method that is based on blockchain for the sharing of the medical records of the patients by ensuring the privacy and the integrity of patients personal data. Immutability of the data of patient is provided by this model and for this it uses the distributed ledger. However if the data size increases it becomes very difficult for blockchain ledger to support it.

In [47][48] given a key management method for the security of the data, but integrity of data is not provided by the proposed method. The key management scheme takes more time for execution and management which makes it not suitable.

K. Croman et al. [49] analyzed some of the metrics for measuring the bitcoin scalability, by the inclusion of the maximum throughput, latency, time for the bootstrapping and the cost per confirmed transaction. In their study they found that the quality of experience is majorly affected by the maximum throughput and the latency.

In [50-52], authors discussed various solutions to enhance the scalability of the blockchain network. Their solutions are mainly based on the problems related to reducing overheads and vertical scaling in the blockchain network. However, they include no information about the sharding which can be a better solution for scaling out the network of blockchain.

In [53-56] the authors discussed the concept of sharding in which the network is divided into subsets called shards. Every shard works in different transaction set rather than the entire network working for the same transaction. In their study, they found that sharding is able to allow the network for scaling the number of shards and to achieve high throughput and storage.

In [16] authors discussed some security issues related to the traditional blockchain system. The safety of conventional cryptographic mechanism majorly based on insolvability of elliptical curve discrete log problem or integer factorization problem. The work done in [57] on quantum computing shows that the quantum computers are having a great speed for computing parallel work which will become a significant threat to the traditional algorithm used for cryptography and hash function. The cryptosystems that uses public key, the data can be recovered fast from future quantum computing attacks. These types of attacks having a major impact on the algorithms with public key system [58-62], that can be broken in polynomial-time with the algorithm given by Shor [63] on an average capable quantum computer. Moreover, quantum computers may use algorithm given by Grover [64] for acceleration of the generation of hashes that enables recreating whole blockchain.

Previously post quantum cryptography is given by many researchers for dealing with the attacks of quantum computing. Specifically, cryptography technique that is lattice-based is most accepted for making quantum computer attack survivor [57]. In [65] author proposed the first lattice-based blind signature scheme based on one-way trapdoor function. Moreover, he also designed the lattice and identity-based signature scheme [66]. In [67] authors proposed a technique for assigning a short lattice basis. The proposed work improves the efficiency of the lattice-based cryptographic scheme by fixing the lattice dimensions. In [68] the authors designed an identity-based encryption technique from lattices. Motivated from the above research and analysis, we consider that lattice-based cryptography can be utilized to increase the blockchain security.

Gao et al. [69], introduced lattice problem-based signature scheme to secure present cryptocurrency scheme. The authors use preimage sampling algorithms for selecting the random value and sing message. Also, a lattice-based

delegation algorithm is used to generate secret keys. Although this work is proposed for the cryptocurrency scheme, however, it can be utilized for storing IoT data using post-quantum blockchain.

The above-related work shows different approaches and techniques to store and protect IoTs data based on cloud and blockchain networks. There are still some issues that need to be addressed which are as follows: • The present IoT data storage framework is based on centralized could architecture a single point of failure and vulnerable to various kinds of attacks.

• It is inefficient for IoT devices to communicate with blockchain network directly as they have low resources. • In present work, IoT devices are authenticated by cryptography techniques over the network, which brings key distribution problem and requires high computation. • The on-chain storage of IoT data, to ensure integrity, makes the network unscalable and decrease the throughput of the blockchain network • A single consensus protocol is being used for all types of transaction. To increase the throughput, application-dependent consensus protocols are required. • The present blockchain technology, which is based on

87% MATCHING BLOCK 4/4 W https://ruc.udc.es/dspace/bitstream/handl ...

public-key cryptosystems and hash functions, are threatened by the evolution of quantum computers in the

near future. So post-quantum cryptography techniques are required to resist quantum attacks.

3. Rationale Nowadays IoT is widely used in, smart houses, smart transport, smart manufacture, smart healthcare systems and many more fields, storing and protecting the huge amount of IoT data is also a challenging issue. In traditional IoT that is cloud-based, structures data is collected and controlled by a central server which causes a single point of failure. Meanwhile, the major dependency on the centralised servers puts major issues of trust and also sensitive data stored on a cloud server can be acquired by the third party without notifying the data owner.

Blockchain with edge computing, in this case, offers a convenient platform to storage and protect IoT data. Blockchain provides decentralized storage without any intervention of the centralized server and ensures traceability and accountability of IoT data. As IoT devices have less storage and computation power Edge computing can be used to overcome the problem. The existing researches of IoT data storage based on blockchain and edge computing do not much focus on the security of data and scalability of blockchain. These opportunities motivate us to propose our research work based on post-quantum blockchain.

4. Objectives The aim of this study is to design a framework for data storage of IoT devices based on post quantum blockchain network with enhanced security. To achieve the aim following objectives are identified.

1. To design an enhanced authentication mechanism for IoT devices over the post quantum blockchain network 2. To design a method for IoT data storage over distributed network using post quantum blockchain.

3. To design a mechanism which improve scalability of post quantum blockchain network.

4. To design a security mechanism using post quantum blockchain to secure the IoT data stored on distributed network.

5. Methodology There are many tools available for implementation of permissioned blockchain some of them are discussed as follows:

• MultiChain

Multichain [70] is a tool for the implementation of blockchain with permission and is also private. It is the extended open source fork of bitcoin. This tool can be used for the launch of some custom blockchains that can be private as well public also its configuration is very easy. For some of the enterprise users and also for the business users this tool provides some inbuilt features and enhancement. Native asst support, huge storage capacity makes it more usable. Here a unique approach is used that works on the basis of permission management for consortium blockchains. Public blockchains are not much efficient. This extensions are achieved while the compatibility maintenance for various technical aspects of Bitcoin Core; hence, much of bitcoin documentation can be applied to the multichain also.

• Hyperledger Fabric Hyperledger fabric [71] is distributed ledger technology (DLT) that is open source and also used for enterprise level. Some of the major points which make it different from available distributed ledgers are as its development is done under linux, which makes it more sustaining and reliable. Support of smart contracts with java, Go, Node.js are

firstly introduced by the fabric distributed ledged platform as compared to the domain specific languages (DSL). This states that many of the enterprises contains the set of skills that is required for the smart contracts development and extra training for the new language or DSL is not compulsory. This platform is permissioned that is as we see in the public permissioned network there is knowledge of every participant to other participant which makes it less trusted platform for working. It means that in a condition where the trust upon each other is not much so we can carry out the work in the provision of any governing model which keeps track of the trust between the participants like the agreement between them or any framework for the dispute handling. It support protocol like pluggable consensus which makes this platform work more effectively for various use cases and trust based models. • R3 CORDA R3 is is institution for finance which built the corda in 2015 for blockchain implementation and made it open source. Corda [72] [73] the cost is reduced by using this platform for cutting edge blockchain and the institutions can work from this platform. This model does not having any token based system or the cryptocurrency by which it becomes permissioned platform so it makes it allowing only authorized individuals and limits them from accessing the whole network. As the model works on the permissioned mode so the safety and privacy of data is on high level which allows the fine grained control to digital records. Initially CORDA is designed for only financial sector but currently it is applied in various industries such as healthcare, supply chain, trade finance and in government works. There are 60 plus firms that makes use of CORDA for the blockchain platform some of the firms are INTEL, MICROSOFT etc. Firms like HSBC, Bank of America Merill Lynch, Intel and many more have invested around $107 million into R3 CORDA.

12